CLAIMS

1. A method for routing data packets for network flow analysis by a multi-processor system having a plurality of processors, comprising:

receiving a data packet, the data packet comprising data sufficient to identify a network connection with which the data packet is associated;

calculating a hash value based on said data sufficient to identify the network connection with which the data packet is associated; and

assigning the data packet based on said hash value to one of said plurality of processors for analysis.

2. The method of claim 1, wherein said data sufficient to identify the network connection with which the data packet is associated comprises address data.

3. The method of claim 1, wherein said data sufficient to identify the network connection with which the data packet is associated comprises address data associated with a source computer that sent the data packet and address data associated with a destination computer to which the data packet is addressed.

4. The method of claim 1, wherein the data packet is sent using the TCP/IP suite of protocols and said data sufficient to identify the network connection with which the data packet is associated comprises an IP address and port number associated with the source computer that sent the data packet and an IP address and port number associated with the destination computer to which the data packet is addressed.

5. The method of claim 1, further comprising storing the data packet in host memory associated with the multi-processor system.

6. The method of claim 5, further comprising sending an interrupt message to a driver, the interrupt message comprising data identifying the storage location in host memory in which the data packet is stored.

7. The method of claim 1, further comprising storing the data packet in host memory associated with the multi-processor system and wherein said step of routing comprises sending to said one of said plurality of processors data identifying the storage location in host memory in which the data packet is stored.

8. The method of claim 7, wherein the step of sending to said one of said plurality of processors data identifying the storage location in host system memory in which the data packet is stored comprises storing said data identifying the storage location in a work queue associated with the processor.

9. The method of claim 8, wherein said work queue is a circular queue.

10. The method of claim 1, further comprising associating the data packet with one or more other data packets associated with the same network connection with which the received data packet is associated to recreate a network flow associated with said network connection.

11. The method of claim 10, further comprising analyzing the network flow to determine if any security-related event has occurred.

12. The method of claim 11, wherein a security-related event is determined to have occurred if the network flow matches a pattern associated with a known attack.

13. The method of claim 11, wherein a security-related event is determined to have occurred if the network flow deviates from normal and permissible behavior under the network protocol under which the data packet was sent.

14. A computer program product for routing data packets for network flow analysis by a multi-processor system, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

receiving a data packet, the data packet comprising data sufficient to identify a network connection with which the data packet is associated;

calculating a hash value based on said data sufficient to identify the network connection with which the data packet is associated; and

assigning the data packet based on said hash value to a processor of said multi-processor system for analysis.

15. A system for routing data packets for network flow analysis, comprising:

a plurality of processors configured to perform network flow analysis;

a network interface card configured to receive data packets via a network connection, each data packet comprising data sufficient to identify a network connection with which the data packet is associated; and

a driver configured to:

calculate a hash value based on said data sufficient to identify the network connection with which the data packet is associated; and

assign the data packet based on said hash value to one of said plurality of processors for analysis.